REMARKS

Reconsideration of the rejections under 35 U.S.C. § 102(b) [claims 50-64 and 66-75] and 35 U.S.C. § 103(a) [claim 65] over the six cited U.S. patent references is respectfully requested in light of these Remarks. No amendments to claims 50 – 75 are being made. Each of the six cited patent references is individually discussed below.

Incidentally, it should be noted that the present application is a continuation claiming priority from an initial parent application filed September 1, 1993, and a continuation-in-part of that application filed November 12, 1993. The present claims, therefore, have an effective filing date of at least as early as November 12, 1993. Section 102(b) is an inappropriate ground for rejecting the claims over U.S. patent nos. 5,357,573 ("Walters") and 5,343,530 ("Viricel") since they were each published after November 12, 1993. Since both of the Walters and Viricel patents were filed in the U.S. in August 1992, prior to the earliest September 1, 1993 date to which the claims herein can be entitled, they will be considered for the purpose of this response as references under 35 U.S.C. § 102(e).

U.S. patent no. 5,357,573 ("Walters")

In Walters, a software program is stored in a memory card along with a protection routine and a comparison code that protect the software program from unauthorized use. The protection routine is run when the software program is accessed through a host to which the memory card is connected. The protection routine compares its comparison code with a protection code stored in the card, either in a separate read-only-memory (ROM) or as part of the main static-random-access-memory (SRAM) or dynamic-random-access-memory (DRAM) that stores the software program. If they compare, the software program is allowed to run on the host; if they do not compare, the protection routine prevents the software program from running on the host.

Although the protection and comparison codes may be encrypted, no suggestion has been found of encrypting the protected software program; it appears to be stored in the memory card without any encoding. Indeed, the Walters patent teaches away from encoding the software program since an advantage of its technique is stated to be that the software program may be executed directly from the memory card without having to be loaded into the memory of the host (col. 4, lns. 27-30), something that would be more difficult if some form of real time decoding of stored encoded data was required.

Therefore, each of the independent claims 50, 63, 66, 67 and 71 of the present patent application is novel over the Walters patent for specifying that the user data are stored on the memory card in an encoded form. All of their dependent claims are thus also novel for the same reason.

Although the ROM within the memory card of the Walters patent that stores the protection code may be a flash memory chip (which is then disabled from altering the protection code), the main memory is disclosed to be either SRAM or DRAM (col. 3, ln. 62 – col. 4., ln. 2). There is this additional item of novelty in those claims that specify the protected data to be stored in a non-volatile or flash memory. These include claims 57, 58 and 66-75.

Another point of novelty is included in claims 61-63, 66 and 71-75 rejected over the Walters patent, namely the use of a mother card including the memory controller. A memory card is removably connectable with the mother card, and the mother card is in turn removably connectable with a host. This group of claims defines the encoding or decoding, or both, of the encoded data stored in the memory card to be performed by the controller in the mother card. The Office Action (paragraph bridging pages 2 and 3), however, takes the position that the motherboard of the Walters system is the claimed mother card, and that it is inherent that the memory card would be moved between hosts during production and use. Since this requires taking Official Notice of disclosure not in the Walters patent, this ground of rejection is also respectfully traversed.

Claims 61, 63 and 66 specify that the mother card is removably connected with the host. The Walters patent does not even mention a computer motherboard, let alone that it is removable in the manner claimed. Such disclosure cannot be considered to be inherent.

Independent claims 63 and 66 are particularly detailed about the use of the mother card. Data are encoded and written onto the memory card from one host and read and decoded when the memory card is connected to a second host. The mother card is used with one of the hosts but not the other. The Walters patent does not even come close to suggesting this detailed method, nor does the Office Action contend it does.

With regard to claims 71 – 75, the mother card is defined to include a receptacle for receiving a memory card. Walters does not describe any type of motherboard, so certainly does not suggest a motherboard with a memory card receptacle on it. Such a detail cannot be considered inherent in Walters, which does not even use the word "motherboard."

U.S. Patent No. 5,093,731 ("Watanabe et al.")

The Watanabe et al. patent does describe use of a memory card 1 with a camera 10 (dependent claim 64 defines the host to be a camera) but, it is respectfully submitted, does not suggest fundamental limitations of the claims. For example, nothing has been found in Watanabe et al. about storing its picture data in an encoded form, and there is therefore nothing about storing "information useful to decode" such data in the memory card. Since both of these limitations are part of each of the rejected claims 50 – 70, the Watanabe et al. patent cannot be held anticipate them.

There are two items of information described by Watanabe et al. to be stored along with the picture data. The data of one picture and this other information are stored in an individual one of the memories 2. One information item is a "recording sequence code" which is simply a sequential number from the camera of the picture stored in the memory. The second item of information is a "recording-finished code" which is "data indicating whether a recording has been made" (col. 3, lns. 54-55); that is, in the nature of a flag indicating whether there is picture data stored in the one of the memories 2 in which the code is stored. So even if the picture data stored in the memory card are somehow argued to be encoded, even though not described in Watanabe et al. to be encoded, there is no information stored along with the picture data that is "useful to decode" (claim 50) such data.

There are other features of the claims not suggested by the Watanabe et al. patent and not mentioned in the Office Action, such as the use of a mother card defined by rejected claims 61 – 64 and 66. Independent claims 63 and 66 are particularly specific on the use of a mother card with a memory card that is connected with two different hosts at different times. Nothing even remotely suggesting these detailed methods are seen to be disclosed by the Watanabe et al. patent.

Further, no suggestion of the details of the mother card of claims 71 and 72 are found in the Watanabe et al. patent. The term "motherboard" cannot even be found in the Watanabe et al. patent, and there is certainly not any discussion of anything remotely resembling the mother card of claims 71 and 72.

U.S. Patent no. 4,935,962 ("Austin")

Austin's first embodiment, upon which the Office Action seems to rely, is a technique of authenticating the card 30 (Figure 2). The issuer of the card 30 calculates a series of values S_1 . . S_n from a public value N and a secret key d, and then stores the values S_1 . . S_n in the secure memory 42, along with the public value N. (Col. 5, ln. 58 – col. 6, ln 12.) To authenticate the card, the card acceptor device 32, to which the memory card 30 is connected, generates a random number v and sends it to the card. The card then calculates Y from v, N and S_1 . . S_n, and sends Y to the acceptor device 32. The acceptor device 32 then makes a calculation from the public values F_1 . . F_n, N and v, and makes a further calculation from the value Y received from the card. By comparing two values resulting from the calculations, the acceptor device 32 then determines whether the card is authentic (col. 8, ln. 40 – col. 7, ln. 13).

It is not understood how this could possibly anticipate the present application claims. No data are described to be stored in the memory card, with which all the rejected claims 50 – 63 and 66 – 70 are directed. None of the card authenticating values N and S_1 . . S_n that are stored on the memory card 30 are said to be encrypted. Indeed, the only portion of the Austin patent referenced in the Office Action to discuss data encoding or decoding is a Background discussion (col. 1, ln. 61 – col. 2, ln. 8) of public key cryptography, after which it is dismissed as ". . not practical for low cost replicated entities." (col. 2, lns. 28-29.) An improvement then described by Austin is much different and does not involve storing encoded data on the memory card.

A second embodiment described with respect to Figure 4 of the Austin patent (begins at col. 7, ln. 51) stores a message M on a memory card 30A that is authenticated by appending an authentication code (certificate) to the message. Neither the message M or the authentication code appear to be encoded in any manner.

Nothing has been found discussed in the Austin patent to anticipate any of the rejected application claims 50-63 and 66-70. The memory cards described in the Austin patent appear to be designed to give access of an individual to an electronic system. This access is granted only after the authenticity of the card is verified. This is quite different than the present application claims where data are stored on a memory card in an encoded way, along with information on how to decode the data.

There are other features of the claims not suggested by the Austin patent and not mentioned in the Office Action, such as the use of a mother card defined by rejected claims 61 –

63 and 66. Independent claims 63 and 66 are particularly specific on the use of a mother card with a memory card that is connected with two different hosts at different times. Nothing even remotely suggesting these detailed methods is seen to be disclosed by the Austin patent.

U.S. Patent No. 4,656,474 ("Mollier et al.")

The Mollier et al. patent describes a technique of authenticating the signature of a signed message that has been received. The signature is attached to the message to authenticate it but no mention of encrypting the message has been found. This is confirmed by the three passages of the Mollier et al. patent referenced in the Office Action. Parameters stored in memory along with data of the message M are used by the sender to form an identification I which is characteristic of the sender. The identification I is joined with the message M and sent.

It seems clear that the Mollier et al. patent does not suggest storing user data in a memory in an encoded form along with information useful to decode it, as defined by the rejected claims. It is respectfully submitted that the Office Action (page 4, lns. 12-19) is in error in stating that the Mollier et al. patent discloses storing message data M in an encoded form and uses information stored with it to decode the message data. Rather, the portions of the Mollier et al. patent specifically cited in the Office Action discuss sending the message M with an identification I that authenticates the message, not that provides the recipient information necessary to decode the message M. No mention of the message M being encoded has been found.

There are also other features of the claims not suggested by the Mollier et al. patent and not mentioned in the Office Action, such as the use of a mother card defined by rejected claims 61 – 63 and 66. Independent claims 63 and 66 are particularly specific on the use of a mother card with a memory card that is connected with two different hosts at different times. Nothing even remotely suggesting these detailed methods is seen to be disclosed by the Mollier et al. patent.

U.S. Patent No. 4,816,651 ("Ishording")

Similarly, no suggestion has been found in the cited Ishording patent of storing its data INF in an encoded form in a memory card (on the right of Figure 1) along with information useful to decode the data, as claimed. Rather, the data INF are encoded in the course of a

processing device (on the left of Figure 1) reading the data INF from the memory card. As shown in Figure 2 for reading data from the memory card, the data INF are encoded by a number X randomly generated in the processing device and sent to the memory card after being encoded with a key SK stored in both the memory card and processing device. The encoded data are then decoded in the processing device by use of the random number X that it generated. The claimed idea of storing encoded data along with information useful to decode the data is not present. The data INF are not described in the Ishording patent to be stored in an encoded form in the memory card but rather are encoded with a number generated by the processing device only when the data INF are read from the memory card.

Further, there are other features of the claims not suggested by the Ishording patent and not mentioned in the Office Action, such as the use of a mother card defined by rejected claims 61 – 63 and 66. Independent claims 63 and 66 are particularly specific on the use of a mother card with a memory card that is connected with two different hosts at different times. Nothing even remotely suggesting these detailed methods is seen to be disclosed by the Ishording patent.

U.S. Patent No. 5,343,530 ("Viricel")

We must similarly respectfully disagree that the Viricel patent "discloses a system for storing both encoded data D and information [key K and algorithm C] useful to the decoding of the data", as alleged in the Office Action (page 5, lns. 3-5). Although an encryption program is stored in the ROM 14 of the memory card 10, no mention has been found that data are stored in the memory card in an encrypted form. Rather, stored data are used along with other parameters to generate an encrypted quantity within the card that is compared with a similar quantity calculated by an attached transaction instrument. The purpose of Viricel is to authenticate the card, not to transfer data from the card.

Other features of the claims not suggested by the Viricel patent and not mentioned in the Office Action include the use of a mother card defined by rejected claims 61 – 63 and 66. Independent claims 63 and 66 are particularly specific on the use of a mother card with a memory card that is connected with two different hosts at different times. Nothing even remotely suggesting these detailed methods is seen to be disclosed by the Viricel patent.

Obviousness Rejection

Claim 65 has not been rejected under 35 U.S.C. § 102(b), as are the remaining claims, but rather under 35 U.S.C. § 103(a) over the Watanabe et al. patent alone. Claim 65 is submitted to be patentable for the same reasons discussed above that render its independent claim 63 patentable over the Watanabe et al. patent. Claims 63 and 65 describe a detailed method of using a memory card with two hosts wherein a mother card is also employed. Nothing like this is suggested in the Watanabe et al. patent or in any of the other 5 cited patents.

New Claims

New dependent claims 76 – 78 are submitted to be patentable over the cited references for the same reasons as their independent parent claim 71, as given above.

New independent claim 79 defines a data storage system that contains encrypted data along with information useful to decrypt the data, discussed above as distinguishing the cited references. Claim 79, and thus also its dependent claims 80 – 82, are therefore not anticipated by the cited references. In addition, claim 79 recites the presence of a memory controller that does the decryption.

Conclusion

In summary, it is respectfully submitted that none of the six cited references discussed above suggest the claimed combination of both encoded data and information useful to decode the data being stored in a memory card or other data storage system.

Accordingly, it is believed that this application is now in condition for allowance and an early indication of its allowance is solicited. However, if the Examiner has any further matters that need to be resolved, a telephone call to the undersigned attorney at 415-318-1163 would be appreciated.

Respectfully submitted,

February 28, 2005

Gerald P. Parsons
Reg. No. 24,486

PARSONS HSUE & DE RUNTZ LLP
655 Montgomery Street, Suite 1800
San Francisco, CA 94111
(415) 318-1160 (main)
(415) 318-1163 (direct)
(415) 693-0194 (fax)

Date